(U) SID Mailbag: Need-to-Share vs Need-to-Know

FROM: SIGINT Communications
Unknown
Run Date: 11/29/2005

Question : (U) The 9-11 commission recommended that the intelligence community transform from a need-to-know mentality to one of need-to-share.

(U//FOUO) How does SID view the recommendation, specifically with regard to information held only within the SIGINT production chain? Will SID directive 406 be rewritten to reflect a sharing responsibility?

Answer:

(U//FOUO) Events of the last several years have clearly demonstrated that the Intelligence Community (IC), and, in fact, the federal government, must do a much better job of sharing information. We talk now more about the need-to-share and are taking great efforts to ensure we share as much information as possible. That said, if we do not want to risk losing intelligence sources, we must still be certain to protect those sources and the methods by which we collect intelligence. Therefore, the need-to-know concept remains alive and well-- but we understand it now more as a need-to-know in a need-to-share environment.

(U//FOUO) The need-to-share change must happen not only outside the SIGINT production chain, but also within it. We have already transformed SID Management Directive 406 into USSID CR1610 with a specific annex titled "Raw SIGINT Database Access Procedures for Extended Enterprise SIGINT Production Personnel." This document is an effort to simplify getting database accesses within the SIGINT Production Chain, something that has been a challenge at times. Because Executive Order (EO) 12333 and National Security Council Intelligence Directive (NSCID) 6 have not been substantially changed since 9/11, we are still bound by those foundational documents to ensure oversight of unminimized and unevaluated or "raw" SIGINT (as defined in USSID CR1610). This means that we must continue to control access to that data. We are in fact granting more and more IC partners access to the data by placing them under SIGINT authorities or integrating more NSA SIGINTers into our partners' operations to serve those partners in a more timely and targeted way. But we are still bound by the oversight requirements and cannot grant wholesale access.

(U//FOUO) We also now have NSA/CSS Policy 1-9 on Information Sharing that implements IC and other executive branch directives on information sharing and clarifies what SIGINT (and Information Assurance) information may be shared and with whom. That policy is available here. The SIGINT Policy office, together with other SID elements, is currently working to develop more detailed implementation guidelines for metadata sharing so that SID analysts will better understand exactly what can be shared with whom.

(C) We have also tried some efforts to grant SIGINT authorities to larger sets of partners, such as the Joint Task Force-CT, where we worked with more than 30 DIA Counterterrorism (CT) analysts to get them access to a set of CT-related databases. We had to work through a number of problems in this effort -- one was the amount of bandwidth needed to access and pull the data and other problems were related to hardware/server issues. Another problem involved the training needed to understand the data in our databases and how to work with it and verify it.

(U//FOUO) The various pilot efforts we have undertaken with selected partners have underlined the very real value of collaborating with those partners on the data we share with them. Consequently, in the interest of improving SIGINT analysis, analysts are encouraged to share with our partners previously unpublished SIGINT information that has been minimized and evaluated for foreign intelligence. USSID CR 1611(P) provides details of those procedures and responsibilities. (See related article "Pre-Pub Sharing of SIGINT: An Everyday Event .)

(U//FOUO) Because data access is not only a policy matter, we have also been working with the SIGINT Contact Center to devise an expedited process, especially for tactical SIGINTers, to allow access to needed databases. We are working with ITD to facilitate approval for NSA WEBWORLD access across the IC.

(U//FOUO) Please direct further questions on this topic to [redacted] S02L1, SIGINT Policy.
